A Moving Target Defense for Data Storage Devices
April 28, 2023

Executive Summary

This white paper serves to provide pertinent background information to both public sector and private sector entities in advance of Technical Interchange Meetings (TIMs) with NexiTech. Efforts are currently underway to identify partners that wish to collaborate with NexiTech on research and development projects that seek to further refine the patented Intellectual Property (IP) previously developed by NexiTech in the nascent Storage Security domain and then integrate it into their own product portfolios.

This emerging technology provides NexiTech's partners the opportunity to significantly strengthen their positions in Storage Security, a very important field that bridges the gap between Data Storage and Cyber Security. Gartner has coined the term "CyberStorage" to mean the same thing. The innovative technology under consideration here provides enhanced protection for data-in-flight and also effective protection from ransomware. Gartner has declared that 2023 is going to be "the year of Moving Target Defense". These entities can cement leadership positions in CyberStorage by partnering with NexiTech, a leading authority on Moving Target Defense.

Problem Statement

By now everybody knows ransomware is a scourge that has been around for years and is only getting worse. We hear about so many data breaches and cyber attacks and serious threats to critical infrastructure on a daily basis that it seems we're becoming numb to it. The data storage community is finally waking up to the fact that much more can be done, and more must be done to stop criminals from harming innocent people.

But cyber security is hard. True "security" only exists when a holistic approach is taken that embraces a wide range of technologies, applied at a number of different layers, and when specific technologies are chosen that match the requirements of a certain customer or application. The technology you are about to preview is a new and different approach to protecting data in motion. It provides an additional layer of security for data storage devices and appliances and therefore enhances the cyber security posture of data storage by providing greater defense in depth.

Active Cyber Defense

Modern computing systems are, for the most part, static in nature. That makes them easy to attack and hard to defend. Attackers have all the time in the world to plan an attack at the time and place of their choosing, and that gives them an asymmetric advantage.

Active Cyber Defense, or Dynamic Defense (also known as Moving Target Defense), seeks to introduce controlled change and uncertainty to multiple network and system dimensions. This serves to decrease the attacker's window of opportunity and increase the economic costs of the attacker's probing and attack efforts. That takes away their asymmetric advantage and also renders the attacker’s surveillance obsolete.

Moving Target Defense for Data Storage Devices

We use storage virtualization to instantiate multiple abstractions of a data storage device. We also change the device type. Virtual tape is an example of a technology in which a disk device is made to look like a tape device. We make the disk device look like a generic or unknown device. We have "cloaked" the device by changing its device type. The host operating system now has no idea how to talk to the device because it is no longer a disk drive. This, alone, is an effective ransomware protection, because most ransomware attacks depend on the fact that there is a usable file system on the disk. Where there is no file system, there can be no ransomware attack.

By creating multiple abstractions of the device, we've essentially created multiple virtual communication channels, or virtual ports, for the device. This results in multiple instantiations of the device inside the host computer. At any given point in time, there is only one port that is the "correct" or "active" port. By dynamically, or randomly, changing the configuration of the active port, we create a Moving Target Defense, not unlike that which may be found in today's software-defined networks (IP-hopping) and in yesterday's radio communications (frequency-hopping).

In addition, we also obfuscate the command set. Changing the command set for the device makes it more difficult for an attacker to access the device, but not impossible, as this is merely a "covert but static" approach. A determined attacker could still monitor the interface and over time eventually infer the meaning of the commands. For greater security, we implement a multi-dimensional Moving Target Defense. Changing the communications channel from one command to the next defeats the attacker who has taken the time to decode the custom command set. But changing the command set itself from one command to the next makes the approach even more dynamic by changing two dimensions of the attack surface at once. The two communicating entities, the initiator and the target, are kept in sync with one another with respect to what channel is being used, and we also randomly change the command set. In summary, we're changing multiple dimensions of the attack surface, and we're doing this in an autonomous manner, and that creates a Moving Target Defense which is unpredictable to adversaries. The result is an autonomous system that randomly changes multiple dimensions of the attack surface, making it unpredictable to adversaries.

What About Encryption?

Encryption is an essential cyber security technology that protects data when a device is lost or stolen. Self Encrypting Drives (SEDs) protect data-at-rest, but not data-in-motion. Ransomware is not mitigated by SED technology because the data are encrypted only after arriving at the storage device (with WRITE commands), then decrypted before leaving the storage device (with READ commands). In a Ransomware attack, Malware is inserted into a system at a much higher layer in the system (at the Application layer). Requests to access the storage media that come from the Malware application are indistinguishable to the storage device from regular requests. With Ransomware, user data are encrypted at the application level by the Malware application, then sent down to the storage device, where they are re-encrypted before being written on the storage media. In summary, SEDs protect data-at-rest, but not from malware or network attacks.

Now let's talk about data-in-motion, where the data are in transit from point A to point B, for example, when flowing across the storage device interface or storage area network. Isn't encryption used here as well? Yes, absolutely, it is (or can be). This is known as Link Encryption or Secure Channel, and protocols that provide this type of protection are addressing some of the same types of threats that Moving Target Defense addresses, albeit in different ways. These threats are:

Sniffing/Snooping of storage traffic (man-in-the-middle attacks)
Masquerading/Spoofing (man-in-the-middle attacks)
Ransomware
Session Hijacking

There are several Storage Area Network (SAN) protocols that provide Link Encryption:

iSCSI	Internet Protocol security	IPsec
Fibre Channel	Fibre Channel Security Protocol	FC-SP-2
NVMe-oF	Transport Layer Security	TLS 1.3

However, encrypting data on the wire does not by itself protect against ransomware nor against physical theft of the storage system because the data are decrypted on both ends of the link, upon arrival at the storage server (target) and at the storage client (initiator).

NIST Cybersecurity Framework (CSF)

The National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework) organizes basic cybersecurity activities into the following functions: Identify, Protect, Detect, Respond and Recovery. While many cybersecurity products on the market today tend to focus on Detection and Response, the technology described herein (MTD) provides Protection. Moving Target Defense is, by definition, a proactive form of cyber defense that seeks to prevent attacks before they occur. When used in conjunction with other techniques that Detect and Respond, the total system achieves a greater level of defense in depth.

Is This Really Necessary?

All technologies have pros and cons, including Moving Target Defense (MTD). Framing the conversation in terms of "which is better, encryption or MTD?" is the wrong question. It's not a competition. They are two different technologies that complement one another. They play on the same team. Saying you don't need MTD because you already have encryption is like being a football coach who says he doesn't need a kicker because he already has a good quarterback. They satisfy different requirements and are useful in different situations. Taken together, they make the team stronger. In this case, the goal is to enhance the cyber security posture of the entire system by providing defense in depth.

Topics We Did Not Get Into In This Brief Introduction

1.) Interoperability issues and solutions.
2.) Our existing "proof of concept" demonstration.
3.) Encryption alone may not cut it in the quantum computing era.
4.) Quantum-Resistant (QR) Algorithm Requirements for National Security Systems.
5.) Integration with existing SIEM/XDR solutions.
6.) A detailed discussion of the threat landscape, including management interfaces.
7.) Challenges associated with managing keys, secrets, passphrases and certificates.
8.) Potential "fringe security" markets that are interested in defense in depth include:

Defense
Energy
Finance
Government
Health Care

Conclusion

With this brief introduction, we hope to start a conversation regarding how NexiTech and potential partners may work together to further refine the patented technology described herein. Gartner has declared 2023 is going to be "the year of Moving Target Defense". In addition, a team of more than a dozen Gartner security analysts recently concluded "The Future of Cyber Is Automated Moving Target Defense" and that this emerging technology is a game-changer for improving cyber defense (1). NexiTech was named in the report as the only provider of this technology in the data storage industry, and will appear in an upcoming report whose focus is on technical innovators. Public and private sector entities can cement leadership positions in CyberStorage by partnering with NexiTech, a leading authority on Moving Target Defense.

For more information, please visit www.nexitech.com.

(1) Emerging Tech: The Future of Cyber Is Automated Moving Target Defense